Amendment to the Specification:

Please amend paragraph **[0001]** appearing on page 1 as follows:

> This present application claims priority to United States Provisional Patent Application No. 60/477,921 ~~60/447,921~~ filed on June 13, 2003; United States Provisional Patent Application No. 60/416,583 ~~60/414,586~~ filed on October 8, 2003; and United States Provisional Application No. 60/422,474 filed October 31, 2002. The contents of these three provisionals are incorporated herein by reference in their entirety. The present application is related to U.S. Patent Application No. 10/679,371 ~~10/xxx,xxx~~, entitled "Localized Network Authentication and Security Using Tamper-Resistant and Keys," and U.S. Patent Application No. 10/679,268 ~~10/xxx,xxx~~, entitled "Shared Network Access Using Different Access Keys," both of which are filed concurrently herewith.

Please amend paragraph **[0029]** appearing on page 7 as follows:

> The present invention provides, *inter alia*, a secure, local edge method and system of tracking and enforcing a user's network usage and allowing the user's device to automatically provide feedback to the user as to the user's usage without requiring network access or a connection to a remote server. As the following describes in enabling detail, the invention is generally realized via a combination of software routines and physical keys in the form of easy-to-use adapters that are installed into client computing devices via, for instance, an available USB port. These physical keys are secure, tamper-resistant tokens capable of tracking and enforcing network usage in view of pre-defined conditions and/or limits. In a

preferred embodiment of the invention, the physical keys also facilitate the authentication of the client computing devices on the network and provide secure data communication across the network using, for example, authentication parameters such as one or more cryptographic keys, which are pre-stored in secure storage within the physical keys. For example, an authentication and secure data communications system and method is implemented as described in commonly assigned and corresponding U.S. Patent Applications No. 10/679,371 ~~10/xxx,xxx~~, entitled "Localized Network Authentication and Security Using Tamper-Resistant and Keys," and 10/679,268, ~~10/xxx,xxx~~ entitled "Shared Network Access Using Different Access Keys," filed concurrently herewith, the disclosures of which are incorporated in their entirety herein by reference. In an alternative embodiment, other types of cryptographic authentication and/or data security techniques may be implemented such as, but not limited to a Public Key Infrastructure (PKI). In yet another embodiment, Wired Equivalent Privacy (WEP) is implemented in place of any authentication or data security system and method facilitated by the physical keys.